5. Math 235 Fall 2021, Worksheet 5: p-valuations

On this worksheet, we will see how prime numbers and p-valuations can help solve problems in number theory.

As before, $\mathbb{N}$ means the set $\{0, 1, 2, \ldots\}$.

5.1. Primes

We recall that an integer p is said to be *prime* if it is greater than 1 and its only positive divisors are 1 and p. Thus, the first 10 primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$. An integer that is prime is also called a *prime number* or, for short, a *prime*.

The following properties of primes are well-known (see, e.g., [Grinbe20, §9.1.2 and §9.1.3]):[1]

Proposition 5.1.1. Each integer $n > 1$ has at least one prime divisor.

Proposition 5.1.2. There are infinitely many primes.

Proposition 5.1.3. Let p be a prime. Then, each $i \in \{1, 2, \ldots, p-1\}$ is coprime to p.

Proposition 5.1.4. Let p be a prime. Let $a \in \mathbb{Z}$. Then, we have either $p \mid a$, or the integer p is coprime to a.

Proposition 5.1.5. Let p be a prime. Let $a, b \in \mathbb{Z}$ satisfy $p \mid ab$. Then, $p \mid a$ or $p \mid b$.

A crucial property of primes is that they are the "multiplicative building blocks" of all positive integers. In other words:

Theorem 5.1.6 (Fundamental Theorem of Arithmetic)**.** Let n be a positive integer. Then, n can be represented as a product of primes. Moreover, this representation is unique up to the order of the factors.

For instance, the integer 200 can be represented as a product of primes as follows:

$$200 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5.$$

Of course, the factors in this product can be reordered at will (e.g., we can get $200 = 2 \cdot 5 \cdot 2 \cdot 5 \cdot 2$). Theorem 5.1.6 yields that except for such reordering, there is no other way to write 200 as a product of primes.

Note that Theorem 5.1.6 is perfectly valid for $n = 1$; in this case, the product is empty (and thus equals 1 by definition).

[1] Recall that an integer a is said to be *coprime* to an integer b if $\gcd(a, b) = 1$.

Theorem 5.1.6 is [Grinbe20, Theorem 9.2.5]; its proof can be found in any text on elementary number theory (and many others[2]). Alternatively, you can treat it as an exercise (hint: use Proposition 5.1.1 for the existence part, and Proposition 5.1.5 for the uniqueness).

The representation of a positive integer n as a product of primes is called the *prime factorization* of n. (The definite article is more-or-less justified by the uniqueness part of Theorem 5.1.6.)

5.2. p-valuations

We shall now introduce the notion of the "p-valuation" of an integer n (where p is a prime). Roughly speaking, this is counting how often n can be divided by p without remainder, or, equivalently, how often p appears in the prime factorization of n (when n is positive). Here is the formal definition:

Definition 5.2.1. Let p be a prime.

(a) Let n be a nonzero integer. Then, $v_p(n)$ shall denote the largest $m \in \mathbb{N}$ such that $p^m \mid n$. This is well-defined (see [Grinbe19, Lemma 2.13.22] for a detailed proof). This nonnegative integer $v_p(n)$ will be called the *p-valuation* (or the *p-adic valuation*) of n.

(b) We extend this definition of $v_p(n)$ to the case of $n = 0$ by setting $v_p(0) := \infty$. Here, ∞ is a new symbol ("positive infinity") that is supposed to model an "infinitely large number"; to some extent, we can do basic arithmetic with it (using the rules $k + \infty = \infty + k = \infty$ and $k < \infty$ for all integers k, as well as $\infty + \infty = \infty$), as long as we don't involve it in subtraction, multiplication or division. (See [Grinbe20, Definition 9.3.1 **(b)**] for the details of what can and what cannot be done with ∞.)

Example 5.2.2. **(a)** We have $v_3(18) = 2$. Indeed, 2 is the largest $m \in \mathbb{N}$ such that $3^m \mid 18$ (because $3^2 \mid 18$ but $3^3 \nmid 18$).

(b) We have $v_3(14) = 0$. Indeed, 0 is the largest $m \in \mathbb{N}$ such that $3^m \mid 14$ (because $3^0 \mid 14$ but $3^1 \nmid 14$).

(c) We have $v_3(51) = 1$ and $v_3(54) = 3$.

(d) We have $v_3(0) = \infty$ (by Definition 5.2.1 **(b)**).

Let us now collect some properties of p-valuations. Almost all of them are easy to prove, and all the proofs can be found in [Grinbe20, §9.3.1 and §9.3.2]:

Lemma 5.2.3. Let p be a prime. Let $i \in \mathbb{N}$. Let $n \in \mathbb{Z}$. Then, $p^i \mid n$ if and only if $v_p(n) \geq i$.

[2] In particular, it appears in [Grinbe20, §9.2].

Corollary 5.2.4. Let p be a prime. Let $n \in \mathbb{Z}$. Then, $v_p(n) = 0$ if and only if $p \nmid n$.

Theorem 5.2.5. Let p be a prime.

(a) We have $v_p(ab) = v_p(a) + v_p(b)$ for any two integers a and b.

(b) We have $v_p(a+b) \geq \min\left\{v_p(a), v_p(b)\right\}$ for any two integers a and b.

(c) We have $v_p(1) = 0$.

(d) We have $v_p(q) = \begin{cases} 1, & \text{if } q = p; \\ 0, & \text{if } q \neq p \end{cases}$ for any prime q.

Corollary 5.2.6. Let p be a prime. Let $a_1, a_2, \ldots, a_k$ be k integers. Then, $v_p(a_1 a_2 \cdots a_k) = v_p(a_1) + v_p(a_2) + \cdots + v_p(a_k)$.

Proposition 5.2.7. Let p be a prime. Let $n \in \mathbb{Z}$. Then, $v_p(|n|) = v_p(n)$.

Corollary 5.2.8. Let p be a prime. Let $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then, $v_p\left(a^k\right) = k v_p(a)$.

Proposition 5.2.9. Let n be a positive integer. Let $n = a_1 a_2 \cdots a_k$ be a prime factorization of n (where $a_1, a_2, \ldots, a_k$ are primes). Let p be a prime. Then,

$$(\text{the number of } i \in \{1,2,\ldots,k\} \text{ such that } a_i = p) = v_p(n).$$

Of course, Proposition 5.2.9 just repeats what we have said just before Definition 5.2.1: The p-valuation of n is the number of times that p appears in the prime factorization of n.

Thanks to Proposition 5.2.9, we can rewrite the prime factorization of a positive integer in an "explicit" form, at least if one considers an infinite product that involves p-valuations to be explicit. The infinite product is not as scary as it sounds: It is an infinite product that has only finitely many factors different from 1. Such a product is analogous to an infinite sum that has only finitely many addends different from 0; it is always well-defined, because a factor that equals 1 does not affect the product (just like an addend that equals 0 does not affect the sum).

Theorem 5.2.10 (canonical factorization, or explicit prime factorization)**.** Let n be a nonzero integer. Then:

(a) We have $v_p(n) = 0$ for every prime $p > |n|$. (Note that "for every prime $p > |n|$" is shorthand for "for every prime p satisfying $p > |n|$".)

(b) The product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ has only finitely many factors different from 1, and thus is well-defined.

(c) We have

$$|n| = \prod_{p \text{ prime}} p^{v_p(n)}.$$

(d) If n is positive, then

$$n = \prod_{p \text{ prime}} p^{v_p(n)}.$$

The expression $n = \prod_{p \text{ prime}} p^{v_p(n)}$ in Theorem 5.2.10 **(d)** is called the *canonical factorization* of n. For example, the canonical factorization of 60 is

$$60 = 2^2 \cdot 3^1 \cdot 5^1 \cdot \underbrace{7^0 \cdot 11^0 \cdot 13^0 \cdot 17^0 \cdot \cdots}_{\substack{\text{all exponents here are 0's,} \\ \text{so all these factors equal 1}}}.$$

Of course, most people would write this as $60 = 2^2 \cdot 3 \cdot 5$ (omitting exponents that are 1, and omitting factors that are 1).

Theorem 5.2.10 is [Grinbe20, Theorem 9.3.17]. Its majestic look should not distract from the fact that it is an easy consequence of Proposition 5.2.9 and Theorem 5.1.6. It is nevertheless quite useful. Some of its consequences (all proved in [Grinbe20, §9.3.3]) are the following:

Proposition 5.2.11. Let n and m be integers. Then, $n \mid m$ if and only if each prime p satisfies $v_p(n) \leq v_p(m)$.

Corollary 5.2.12. Let n and m be two integers. Assume that

$$v_p(n) = v_p(m) \qquad \text{for every prime } p. \tag{1}$$

(a) Then, $|n| = |m|$.

(b) If n and m are nonnegative, then $n = m$.

Corollary 5.2.13. Let n be a nonzero integer. Let a and b be two integers. Assume that

$$a \equiv b \bmod p^{v_p(n)} \qquad \text{for every prime } p. \tag{2}$$

Then, $a \equiv b \bmod n$.

Corollary 5.2.14. For each prime p, let b_p be a nonnegative integer. Assume that only finitely many primes p satisfy $b_p \neq 0$. Let $n = \prod_{p \text{ prime}} p^{b_p}$. Then,

$$v_q(n) = b_q \qquad \text{for each prime } q.$$

Proposition 5.2.11 shows that divisibilities between integers can be proved "one prime at a time". Corollary 5.2.13 says the same about congruences (not surprisingly, since a congruence $a \equiv b \bmod n$ is just a divisibility $n \mid a - b$).

Corollary 5.2.12 **(b)** shows that a nonnegative integer is uniquely determined by its p-valuations for all primes p. Let us use the above to thus determine the gcd and the lcm of several integers through their p-valuations:[3]

Proposition 5.2.15. Let $n_1, n_2, \ldots, n_k$ be finitely many integers, with $k > 0$. Let p be a prime. Then:

(a) We have

$$v_p\left(\gcd\left(n_1, n_2, \ldots, n_k\right)\right) = \min\left\{v_p\left(n_1\right), v_p\left(n_2\right), \ldots, v_p\left(n_k\right)\right\}.$$

(b) We have

$$v_p\left(\operatorname{lcm}\left(n_1, n_2, \ldots, n_k\right)\right) = \max\left\{v_p\left(n_1\right), v_p\left(n_2\right), \ldots, v_p\left(n_k\right)\right\}.$$

You might know this proposition already, since it is simply the way to compute gcds and lcms using prime factorizations[4]. This method of computing gcds and lcms is not the fastest one, since it relies on prime factorizations[5]; but it is helpful for a theoretical understanding of gcds and lcms.

A proof of Proposition 5.2.15 is given in the appendix (Section 5.6).

5.3. Example problems

We shall now see some applications of p-valuations.

Exercise 5.3.1. Let a, b, c be three integers.

(a) Prove that $\gcd\left(a, \operatorname{lcm}\left(b, c\right)\right) = \operatorname{lcm}\left(\gcd\left(a, b\right), \gcd\left(a, c\right)\right)$.

(b) Prove that $\operatorname{lcm}\left(a, \gcd\left(b, c\right)\right) = \gcd\left(\operatorname{lcm}\left(a, b\right), \operatorname{lcm}\left(a, c\right)\right)$.

Solution idea. Both parts of this exercise are known results about gcds and lcms (known as the *distributivity laws for gcd and lcm*), and can be solved without any recourse to prime numbers and p-valuations (see, e.g., [Grinbe19, Second solution

[3] We recall that $\operatorname{lcm}\left(n_1, n_2, \ldots, n_k\right)$ denotes the lowest common multiple (aka least common multiple) of k integers $n_1, n_2, \ldots, n_k$.

[4] Namely: For $\gcd\left(n_1, n_2, \ldots, n_k\right)$, you take each prime to the smallest of the exponents with which it appears in the prime factorizations of $n_1, n_2, \ldots, n_k$. For $\operatorname{lcm}\left(n_1, n_2, \ldots, n_k\right)$, you take each prime to the largest of the exponents with which it appears in the prime factorizations of $n_1, n_2, \ldots, n_k$.

[5] Using the Euclidean algorithm to compute gcds (and then the formula $\gcd\left(a, b\right) \cdot \operatorname{lcm}\left(a, b\right) = |ab|$ to compute lcms using gcds) is faster. (Beware: It is not true that $\gcd\left(a, b, c\right) \cdot \operatorname{lcm}\left(a, b, c\right) = |abc|$. Instead, lcms of more than 2 numbers must be computed by iteration: for instance, $\operatorname{lcm}\left(a, b, c\right) = \operatorname{lcm}\left(a, \operatorname{lcm}\left(b, c\right)\right)$.)

to Exercise 2.13.11] for such solutions). However, by working "one prime at a time" using p-valuations (and Proposition 5.2.15 in particular), they become straightforward. Here is how (see [Grinbe19, First solution to Exercise 2.13.11] for details):

(a) We need to prove that the two numbers $\gcd(a, \operatorname{lcm}(b,c))$ and $\operatorname{lcm}(\gcd(a,b), \gcd(a,c))$ are equal. Since these two numbers are nonnegative integers, it suffices (by Corollary 5.2.12 **(b)**) to show that $v_p(\gcd(a, \operatorname{lcm}(b,c))) = v_p(\operatorname{lcm}(\gcd(a,b), \gcd(a,c)))$ for every prime p.

So let us do this now. Let p be a prime. Let $x := v_p(a)$ and $y := v_p(b)$ and $z := v_p(c)$. Note that $x, y, z \in \mathbb{N} \cup \{\infty\}$. Now, Proposition 5.2.15 **(a)** yields

$$\begin{aligned} v_p(\gcd(a, \operatorname{lcm}(b,c))) &= \min\left\{ v_p(a), \quad \underbrace{v_p(\operatorname{lcm}(b,c))}_{\substack{=\max\{v_p(b), v_p(c)\} \\ \text{(by Proposition 5.2.15 \textbf{(b)})}}} \right\} \\ &= \min\left\{ \underbrace{v_p(a)}_{=x}, \ \max\left\{ \underbrace{v_p(b)}_{=y}, \underbrace{v_p(c)}_{=z} \right\} \right\} \\ &= \min\{x, \ \max\{y,z\}\}. \end{aligned}$$

On the other hand, Proposition 5.2.15 **(b)** yields

$$\begin{aligned} v_p(\operatorname{lcm}(\gcd(a,b), \gcd(a,c))) &= \max\left\{ \underbrace{v_p(\gcd(a,b))}_{\substack{=\min\{v_p(a), v_p(b)\} \\ \text{(by Proposition 5.2.15 \textbf{(a)})}}} , \quad \underbrace{v_p(\gcd(a,c))}_{\substack{=\min\{v_p(a), v_p(c)\} \\ \text{(by Proposition 5.2.15 \textbf{(a)})}}} \right\} \\ &= \max\left\{ \min\left\{ \underbrace{v_p(a)}_{=x}, \underbrace{v_p(b)}_{=y} \right\}, \ \min\left\{ \underbrace{v_p(a)}_{=x}, \underbrace{v_p(c)}_{=z} \right\} \right\} \\ &= \max\{\min\{x,y\}, \ \min\{x,z\}\}. \end{aligned}$$

Our goal is to show that the left hand sides of these two equalities are equal. Of course, it suffices to show that the right hand sides are equal, i.e., that we have

$$\min\{x, \ \max\{y,z\}\} = \max\{\min\{x,y\}, \ \min\{x,z\}\}. \tag{3}$$

(We note that the equality (3) is not merely sufficient, but also necessary for Exercise 5.3.1 **(a)** to hold, because x, y, z can take any values in $\mathbb{N} \cup \{\infty\}$. Thus, there is no risk that we have run into a dead end here.)

How do we prove an equality like (3)? The expert answer would be "this is a tropical polynomial identity" (and such identities can be checked mechanically),

but in our case there is a much easier method: The three "numbers" $x, y, z \in \mathbb{N} \cup \{\infty\}$ (we are putting the word "numbers" in scare quotes because we allow ∞, but this does not cause any problems) must be arranged in one of the six orders

$$x \leq y \leq z, \qquad x \leq z \leq y, \qquad y \leq x \leq z,$$
$$y \leq z \leq x, \qquad z \leq x \leq y, \qquad z \leq y \leq x,$$

which subdivides the problem into six possible cases; in each of these six cases, we can explicitly compute and compare the two sides of (3). Here is a table of the results:

case	$\min\{x,\ \max\{y,z\}\}$	$\max\{\min\{x,y\},\ \min\{x,z\}\}$
$x \leq y \leq z$	x	x
$x \leq z \leq y$	x	x
$y \leq x \leq z$	x	x
$y \leq z \leq x$	z	z
$z \leq x \leq y$	x	x
$z \leq y \leq x$	y	y

.

In each case, we see that $\min\{x,\ \max\{y,z\}\}$ and $\max\{\min\{x,y\},\ \min\{x,z\}\}$ simplify to the same result, so that (3) follows. As explained above, this entails that

$$v_p(\gcd(a, \operatorname{lcm}(b,c))) = v_p(\operatorname{lcm}(\gcd(a,b), \gcd(a,c))).$$

Forget that we fixed p. We thus have shown that

$$v_p(\gcd(a, \operatorname{lcm}(b,c))) = v_p(\operatorname{lcm}(\gcd(a,b), \gcd(a,c)))$$

holds for each prime p. According to Corollary 5.2.12 **(b)**, this entails that we have $\gcd(a, \operatorname{lcm}(b,c)) = \operatorname{lcm}(\gcd(a,b), \gcd(a,c))$. Thus, Exercise 5.3.1 **(a)** is solved.

(Incidentally, there is an alternative way of proving (3), without analyzing all six cases. Indeed, we can WLOG assume that $y \leq z$, since y and z play symmetric roles in (3). Assuming this, we can easily see that $\min\{x,y\} \leq \min\{x,z\}$, so that $\max\{\min\{x,y\},\ \min\{x,z\}\} = \min\{x,z\}$. Thus, (3) rewrites as $\min\{x,\ \max\{y,z\}\} = \min\{x,z\}$. However, this is clear, since $y \leq z$ also implies $\max\{y,z\} = z$. This proof of (3) is short and slick, but our above proof has the advantage of following a surefire strategy.)

(b) This is analogous to our above solution to Exercise 5.3.1 **(a)**, except that gcd and lcm trade places, as do min and max. Instead of (3), we now need to prove the equality

$$\max\{x,\ \min\{y,z\}\} = \min\{\max\{x,y\},\ \max\{x,z\}\}.$$

We could again prove this by building a table; alternatively, we could obtain this by applying (3) to $-x$, $-y$ and $-z$ instead of x, y and z (because $\min\{-u,-v\} =$

$-\max\{u,v\}$ and $\max\{-u,-v\} = -\min\{u,v\}$ for any reals u, v). (Now, of course, we need a symbol $-\infty$.) This solves Exercise 5.3.1 **(b)**. □

The following exercise generalizes the fact that $\sqrt{2}$ is irrational (why?):

Exercise 5.3.2. Let k be a positive integer. Let w be a rational number such that w^k is an integer. Prove that w is an integer.

Solution idea. (See [Grinbe20, Exercise 9.3.2] for details.) If $w = 0$, then this is obvious. Thus, we WLOG assume that $w \neq 0$.

The number w is rational. Thus, we can write w in the form $w = m/n$ for some integers m and n with $n \neq 0$. Consider these m and n. Note that $m = nw$ (since $w = m/n$) and thus $m \neq 0$ (since $n \neq 0$ and $w \neq 0$).

From $w = m/n$, we obtain $w^k = (m/n)^k = m^k/n^k$. Hence, m^k/n^k is an integer (since w^k is an integer). Thus, $n^k \mid m^k$.

However, Proposition 5.2.11 (applied to n^k and m^k instead of n and m) shows that $n^k \mid m^k$ if and only if each prime p satisfies $v_p\left(n^k\right) \leq v_p\left(m^k\right)$. Since we have $n^k \mid m^k$, we thus conclude that

$$\text{each prime } p \text{ satisfies } v_p\left(n^k\right) \leq v_p\left(m^k\right). \tag{4}$$

Now, let p be a prime. Then, $v_p(n)$ and $v_p(m)$ are integers (since $n \neq 0$ and $m \neq 0$). Corollary 5.2.8 yields $v_p\left(n^k\right) = kv_p(n)$ and $v_p\left(m^k\right) = kv_p(m)$. Hence,

$$\begin{aligned} kv_p(n) &= v_p\left(n^k\right) \leq v_p\left(m^k\right) \qquad \text{(by (4))} \\ &= kv_p(m). \end{aligned}$$

Dividing this inequality by k, we obtain $v_p(n) \leq v_p(m)$ (since k is positive).

Forget that we fixed p. Thus, we have shown that each prime p satisfies $v_p(n) \leq v_p(m)$. According to Proposition 5.2.11, this entails that $n \mid m$. Hence, w is an integer (since $w = m/n$). This solves Exercise 5.3.2. □

Exercise 5.3.3. Let n be a positive integer.

(a) Prove that

$$(\text{the number of positive divisors of } n) = \prod_{p \text{ prime}} \left(v_p(n) + 1\right).$$

(The product on the right hand side is infinite, but it is well-defined, since only finitely many of its factors differ from 1.)

(b) Prove that the number of positive divisors of n is even if and only if n is not a perfect square.

(A *perfect square* means the square of an integer.)

Solution idea. **(a)** (See [Grinbe19, Proposition 2.18.1 **(b)**] for details.) Let $n = 2^\alpha 3^\beta 5^\gamma \cdots$ be the canonical factorization of n; thus, $\alpha = v_2(n)$ and $\beta = v_3(n)$ and $\gamma = v_5(n)$ and so on.[6] Hence, $\prod_{p \text{ prime}} \left(v_p(n) + 1\right) = (\alpha+1)(\beta+1)(\gamma+1)\cdots$. Thus, we must prove that

$$(\text{the number of positive divisors of } n) = (\alpha+1)(\beta+1)(\gamma+1)\cdots. \tag{5}$$

Using Proposition 5.2.11, we can easily see that any positive divisor of n has the form $2^{\alpha'}3^{\beta'}5^{\gamma'}\cdots$ for some sequence[7]

$$(\alpha', \beta', \gamma', \ldots) \in \{0,1,\ldots,\alpha\} \times \{0,1,\ldots,\beta\} \times \{0,1,\ldots,\gamma\} \times \cdots$$

(that is, for some $\alpha' \in \{0,1,\ldots,\alpha\}$ and some $\beta' \in \{0,1,\ldots,\beta\}$ and some $\gamma' \in \{0,1,\ldots,\gamma\}$ and so on). Moreover, any choice of sequence

$$(\alpha', \beta', \gamma', \ldots) \in \{0,1,\ldots,\alpha\} \times \{0,1,\ldots,\beta\} \times \{0,1,\ldots,\gamma\} \times \cdots$$

gives a different positive divisor $2^{\alpha'}3^{\beta'}5^{\gamma'}\cdots$ of n (since the prime factorization of a positive integer is unique). Thus, we have found a bijection[8] from the set

$$\{0,1,\ldots,\alpha\} \times \{0,1,\ldots,\beta\} \times \{0,1,\ldots,\gamma\} \times \cdots$$

to the set of all positive divisors of n. Therefore, the bijection principle[9] yields

$$\begin{aligned}
&(\text{the number of positive divisors of } n) \\
&= \left|\{0,1,\ldots,\alpha\} \times \{0,1,\ldots,\beta\} \times \{0,1,\ldots,\gamma\} \times \cdots\right| \\
&= \underbrace{\left|\{0,1,\ldots,\alpha\}\right|}_{=\alpha+1} \cdot \underbrace{\left|\{0,1,\ldots,\beta\}\right|}_{=\beta+1} \cdot \underbrace{\left|\{0,1,\ldots,\gamma\}\right|}_{=\gamma+1} \cdot \cdots \\
&\qquad \left(\begin{array}{c} \text{by the infinite product rule, which says} \\ \text{that } |A_1 \times A_2 \times A_3 \times \cdots| = |A_1| \cdot |A_2| \cdot |A_3| \cdot \cdots \\ \text{for any sets } A_1, A_2, A_3, \ldots \end{array}\right) \\
&= (\alpha+1)(\beta+1)(\gamma+1)\cdots.
\end{aligned}$$

This proves (5). Thus, Exercise 5.3.3 **(a)** is solved.

(b) This can be proved in a nice combinatorial way (see [Grinbe20, solution to Exercise 3.8.3]), but let us derive it from part **(a)** instead. Indeed, we have the

[6] The pedantic reader should imagine that the Greek alphabet is infinite, so that there is one letter for each prime.

[7] We are using the Cartesian product of infinitely many sets here. To recall: If $A_1, A_2, A_3, \ldots$ are infinitely many sets, then $A_1 \times A_2 \times A_3 \times \cdots$ means the set of all sequences $(a_1, a_2, a_3, \ldots)$ with $a_1 \in A_1$ and $a_2 \in A_2$ and $a_3 \in A_3$ and so on.

[8] i.e., bijective map

[9] The *bijection principle* says that if there is a bijection from a set X to a set Y, then $|X| = |Y|$.

following chain of logical equivalences:

$$\begin{aligned}
&\left(\text{the number of positive divisors of } n \text{ is even}\right) \\
&\iff \left(\prod_{p \text{ prime}} \left(v_p\left(n\right)+1\right) \text{ is even}\right) \qquad \left(\text{by Exercise 5.3.3 } \textbf{(a)}\right) \\
&\iff \left(v_p\left(n\right)+1 \text{ is even for at least one prime } p\right) \\
&\qquad\qquad \left(\begin{array}{c}\text{since a product of integers is even if and only if} \\ \text{at least one of its factors is even}\end{array}\right) \\
&\iff \left(v_p\left(n\right) \text{ is odd for at least one prime } p\right) \\
&\iff \left(n \text{ is not a perfect square}\right).
\end{aligned}$$

The last "$\iff$" arrow here might need some justification. It is easier to prove the contrapositive – i.e., to prove the equivalence

$$\left(v_p\left(n\right) \text{ is even for all primes } p\right) \iff \left(n \text{ is a perfect square}\right).$$

The "$\implies$" direction of this equivalence follows from Theorem 5.2.10 **(d)**, whereas the "$\impliedby$" direction follows from Corollary 5.2.8. (Convince yourself of all of this!) □

In the next exercise, we will use the notation $[j]$ for the set $\{1, 2, \ldots, j\}$ whenever $j \in \mathbb{N}$.

Exercise 5.3.4. Let n and u be positive integers. Let $a_1, a_2, \ldots, a_u$ be any integers. Set $a_{u+1} = a_1$. Assume that

$$a_i \mid a_{i+1}^n \qquad \text{for each } i \in [u].$$

Set $m = n^{u-1} + n^{u-2} + \cdots + n^0$. Prove that

$$a_1 a_2 \cdots a_u \mid \left(a_1 + a_2 + \cdots + a_u\right)^m.$$

Solution idea. In view of Proposition 5.2.11, it suffices to show that each prime p satisfies

$$v_p\left(a_1 a_2 \cdots a_u\right) \leq v_p\left(\left(a_1 + a_2 + \cdots + a_u\right)^m\right).$$

So let p be a prime. Let

$$k_i := v_p\left(a_i\right) \qquad \text{for each } i \in [u+1].$$

Note that $k_{u+1} = k_1$, since $a_{u+1} = a_1$.

We WLOG assume that the smallest of the u "numbers"[10] $k_1, k_2, \ldots, k_u$ is k_u. (This is a valid WLOG assumption, since we can cyclically rotate our u integers

[10]The word "numbers" is in scare quotes, since some of them can be ∞.

$a_1, a_2, \ldots, a_u$ without changing the exercise[11]; and when we do rotate them, their p-valuations $k_1, k_2, \ldots, k_u$ are rotated along with them.)

For each $i \in [u]$, we have $a_i \mid a_{i+1}^n$ (by assumption) and thus (by Proposition 5.2.11 again) $v_p(a_i) \leq v_p\left(a_{i+1}^n\right) = nv_p(a_{i+1})$ (by Corollary 5.2.8). In other words,

$$k_i \leq nk_{i+1} \qquad \text{for each } i \in [u] \tag{6}$$

(since $k_i = v_p(a_i)$ and $k_{i+1} = v_p(a_{i+1})$). This quickly entails

$$k_{u-i} \leq n^i k_u \qquad \text{for each } i \in \{0, 1, \ldots, u-1\} \tag{7}$$

(indeed, check this by induction on i). Now, Corollary 5.2.6 yields

$$\begin{aligned} v_p(a_1 a_2 \cdots a_u) &= v_p(a_1) + v_p(a_2) + \cdots + v_p(a_u) = k_1 + k_2 + \cdots + k_u = \sum_{i=0}^{u-1} \underbrace{k_{u-i}}_{\substack{\leq n^i k_u \\ \text{(by (7))}}} \\ &\leq \sum_{i=0}^{u-1} n^i k_u = \underbrace{\left(n^{u-1} + n^{u-2} + \cdots + n^0\right)}_{=m} k_u \\ &= mk_u. \end{aligned} \tag{8}$$

On the other hand, we claim that $v_p\left(\left(a_1 + a_2 + \cdots + a_u\right)^m\right) \geq mk_u$. The easiest way to prove this is probably the following: Each $i \in [u]$ satisfies $v_p(a_i) = k_i \geq k_u$ (since k_u is the smallest of the u numbers $k_1, k_2, \ldots, k_u$). In other words, each of the u integers $a_1, a_2, \ldots, a_u$ has p-valuation $\geq k_u$, and thus is divisible by p^{k_u}. Hence, the sum $a_1 + a_2 + \cdots + a_u$ of these u integers is also divisible by p^{k_u}. Thus, $v_p(a_1 + a_2 + \cdots + a_u) \geq k_u$. Now, Corollary 5.2.8 yields

$$v_p\left(\left(a_1 + a_2 + \cdots + a_u\right)^m\right) = m \underbrace{v_p(a_1 + a_2 + \cdots + a_u)}_{\geq k_u} \geq mk_u.$$

Combining this with (8), we obtain $v_p(a_1 a_2 \cdots a_u) \leq v_p\left(\left(a_1 + a_2 + \cdots + a_u\right)^m\right)$, which is precisely what we wanted to prove. □

The p-valuation of a factorial is particularly useful, as factorials often end up involved in divisibilities. Here is an "explicit" formula ([Grinbe20, Theorem 9.3.25], or, in an equivalent form, [Grinbe19, Exercise 2.17.2 **(c)**]):[12]

[11] i.e., replace $a_1, a_2, \ldots, a_{u-1}, a_u$ by $a_2, a_3, \ldots, a_u, a_1$, respectively

[12] Recall: If r is any real number, then $\lfloor r \rfloor$ is defined to be the largest integer that is $\leq r$. This integer $\lfloor r \rfloor$ is called the *floor* of r. Equivalently, $\lfloor r \rfloor$ can be described as the unique integer z satisfying $z \leq r < z + 1$. For instance, $\lfloor 2.2 \rfloor = \lfloor 2.8 \rfloor = \lfloor 2 \rfloor = 2$ and $\lfloor -3.1 \rfloor = \lfloor -\pi \rfloor = \lfloor -4 \rfloor = -4$.

Theorem 5.3.1 (de Polignac's formula)**.** Let p be a prime. Let $n \in \mathbb{N}$. Then,

$$v_p(n!) = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

(The summation sign "$\sum\limits_{i \geq 1}$" is shorthand for "$\sum\limits_{i \in \{1,2,3,\ldots\}}$". The sum $\sum\limits_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor$ in this equality is well-defined, since it has only finitely many nonzero addends.)

Example 5.3.2. Applying Theorem 5.3.1 to $n = 42$ and $p = 5$, we obtain

$$\begin{aligned} v_5(42!) &= \sum_{i \geq 1} \left\lfloor \frac{42}{5^i} \right\rfloor = \underbrace{\left\lfloor \frac{42}{5^1} \right\rfloor}_{=\lfloor 8.4 \rfloor = 8} + \underbrace{\left\lfloor \frac{42}{5^2} \right\rfloor}_{=\lfloor 1.68 \rfloor = 1} + \underbrace{\left\lfloor \frac{42}{5^3} \right\rfloor}_{=\lfloor 0.336 \rfloor = 0} + \underbrace{\left\lfloor \frac{42}{5^4} \right\rfloor}_{=0} + \underbrace{\left\lfloor \frac{42}{5^5} \right\rfloor}_{=0} + \cdots \\ &= 8 + 1 + 0 + 0 + 0 + \cdots = 9. \end{aligned}$$

Theorem 5.3.1 is known as *de Polignac's formula* or *Legendre's formula*. Here is an outline of a proof (first in an informal way, then formalized):

Proof of Theorem 5.3.1 (sketched). Classically, this is shown by expanding $n!$ as the product $1 \cdot 2 \cdot \cdots \cdot n$ and counting "how many ps come from each factor of this product". To wit, precisely $\lfloor n/p \rfloor$ factors of the product $1 \cdot 2 \cdot \cdots \cdot n$ are multiples of p (namely, $p, 2p, 3p, \ldots, \lfloor n/p \rfloor p$), so that the product is divisible by $p^{\lfloor n/p \rfloor}$. Thus, its p-valuation is at least $\lfloor n/p \rfloor$. However, this undercounts the p-valuation of this product, since some of the multiples of p are actually multiples of p^2, and thus contribute 2 rather than 1 to its p-valuation[13]. Thus, we need to refine our tally $\lfloor n/p \rfloor$ by adding the number of multiples of p^2 that appear in this product. This number is $\lfloor n/p^2 \rfloor$. Thus, the p-valuation of our product is at least $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor$. But we are still undercounting the p-valuation, since some of the multiples of p^2 are actually multiples of p^3 and thus contribute 3 rather than 2. So we need to refine our tally again, and this process goes on indefinitely until all possible powers of p are dealt with. As a result, we conclude that the p-valuation of the product $1 \cdot 2 \cdot \cdots \cdot n$ is

$$\lfloor n/p \rfloor + \left\lfloor n/p^2 \right\rfloor + \left\lfloor n/p^3 \right\rfloor + \cdots = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

But this is precisely the claim of Theorem 5.3.1.

This argument can be made more formal by using a certain neat piece of notation known as the *Iverson bracket notation*. To wit, if $\mathcal{A}$ is any logical statement, then we

[13] We are tacitly using Corollary 5.2.6 here, which lets us compute the p-valuation of a product by adding together the p-valuations of its factors.

define the *truth value* of $\mathcal{A}$ to be the integer

$$[\mathcal{A}] := \begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false.} \end{cases}$$

For example, $[2+2=4] = 1$ but $[2+2=5] = 0$.

Now, it is easy to see that each positive integer k satisfies

$$\left\lfloor \frac{n}{k} \right\rfloor = \sum_{m=1}^{n} [k \mid m]. \tag{9}$$

(Indeed, the right hand side of this equality is a sum of 0's and 1's, and it has a 1 for each $m \in \{1, 2, \ldots, n\}$ that is a multiple of k. Thus, the total value of this sum is the number of multiples of k that belong to $\{1, 2, \ldots, n\}$. But this number is easily seen to be $\left\lfloor \frac{n}{k} \right\rfloor$, which is the left hand side.)

On the other hand, each positive integer m satisfies

$$v_p(m) = \sum_{i \geq 1} \left[p^i \mid m \right]. \tag{10}$$

(Indeed, the right hand side is a sum of 0's and 1's, and it has a 1 for each $i \in \{1, 2, 3, \ldots\}$ that satisfies $p^i \mid m$. However, the number of such i's is $v_p(m)$, because these i's are precisely $1, 2, \ldots, v_p(m)$.)

Now, all that remains to be done is a simple computation: From $n! = 1 \cdot 2 \cdot \cdots \cdot n$, we obtain

$$\begin{aligned} v_p(n!) &= v_p(1 \cdot 2 \cdot \cdots \cdot n) = v_p(1) + v_p(2) + \cdots + v_p(n) \qquad \text{(by Corollary 5.2.6)} \\ &= \sum_{m=1}^{n} \underbrace{v_p(m)}_{\substack{= \sum_{i \geq 1} \left[p^i \mid m \right] \\ \text{(by (10))}}} = \underbrace{\sum_{m=1}^{n} \sum_{i \geq 1}}_{= \sum_{i \geq 1} \sum_{m=1}^{n}} \left[p^i \mid m \right] = \sum_{i \geq 1} \underbrace{\sum_{m=1}^{n} \left[p^i \mid m \right]}_{= \left\lfloor \frac{n}{p^i} \right\rfloor} = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor. \\ &\qquad \text{(by (9), applied to } k = p^i\text{)} \end{aligned}$$

This proves Theorem 5.3.1. □

Here is one of many applications of de Polignac's formula (see [Grinbe20, §9.3] for more):

Exercise 5.3.5. Let $n, a, b \in \mathbb{N}$.

(a) Prove that $\dfrac{(na)!\,(nb)!}{a!b!\,(a+b)!^{n-1}}$ is an integer.

(b) Assume that $n > 0$ and $(a, b) \neq (0, 0)$. Prove that the integer $\dfrac{(na)!\,(nb)!}{a!b!\,(a+b)!^{n-1}}$ is divisible by n.

Solution idea. **(a)** We assume that $n > 0$. (The proof in the case when $n = 0$ is similar, with minor changes.[14]) From $n > 0$, we obtain $n \geq 1$, so that $n - 1 \in \mathbb{N}$. Hence, $(a+b)!^{n-1}$ is an integer.

We must show that $\dfrac{(na)!\,(nb)!}{a!b!\,(a+b)!^{n-1}}$ is an integer. In other words, we must show that $a!b!\,(a+b)!^{n-1} \mid (na)!\,(nb)!$. Because of Proposition 5.2.11 (applied to $a!b!\,(a+b)!^{n-1}$ and $(na)!\,(nb)!$ instead of n and m), this will follow if we can show that each prime p satisfies

$$v_p\left(a!b!\,(a+b)!^{n-1}\right) \leq v_p\left((na)!\,(nb)!\right). \tag{12}$$

Thus, we shall now focus on proving (12).

So let p be a prime. Applying Corollary 5.2.8 and Corollary 5.2.6, we find

$$\begin{aligned}
&v_p\left(a!b!\,(a+b)!^{n-1}\right) \\
&= v_p\left(a!\right) + v_p\left(b!\right) + (n-1)\, v_p\left((a+b)!\right) \\
&= \sum_{i\geq 1}\left\lfloor \frac{a}{p^i}\right\rfloor + \sum_{i\geq 1}\left\lfloor \frac{b}{p^i}\right\rfloor + (n-1)\sum_{i\geq 1}\left\lfloor \frac{a+b}{p^i}\right\rfloor \qquad \text{(by Theorem 5.3.1)} \\
&= \sum_{i\geq 1}\left(\left\lfloor \frac{a}{p^i}\right\rfloor + \left\lfloor \frac{b}{p^i}\right\rfloor + (n-1)\left\lfloor \frac{a+b}{p^i}\right\rfloor\right) \qquad (13)
\end{aligned}$$

[14] Alternatively, it is not hard to solve Exercise 5.3.5 **(a)** in the case when $n = 0$ directly, using binomial coefficients. Namely, assume that $n = 0$. Recall that $\binom{p}{q} = \dfrac{p!}{q!\,(p-q)!}$ for any $p \in \mathbb{N}$ and $q \in \{0, 1, \ldots, p\}$. Applying this to $p = a+b$ and $q = a$, we obtain $\binom{a+b}{a} = \dfrac{(a+b)!}{a!\,((a+b)-a)!} = \dfrac{(a+b)!}{a!b!}$. On the other hand, from $n = 0$, we obtain

$$\begin{aligned}
\frac{(na)!\,(nb)!}{a!b!\,(a+b)!^{n-1}} &= \frac{(0a)!\,(0b)!}{a!b!\,(a+b)!^{0-1}} = \frac{1\cdot 1}{a!b!\,(a+b)!^{-1}} \\
&\qquad (\text{since } (0a)! = 0! = 1 \text{ and } (0b)! = 0! = 1 \text{ and } 0 - 1 = -1) \\
&= \frac{(a+b)!}{a!b!} = \binom{a+b}{a}. \qquad (11)
\end{aligned}$$

However, it is known that $\binom{p}{q}$ is an integer whenever $p \in \mathbb{N}$ and $q \in \mathbb{N}$. Applying this to $p = a+b$ and $q = a$, we conclude that $\binom{a+b}{a}$ is an integer. In view of (11), this rewrites as follows: $\dfrac{(na)!\,(nb)!}{a!b!\,(a+b)!^{n-1}}$ is an integer. Hence, Exercise 5.3.5 **(a)** is solved in the case when $n = 0$.

and

$$\begin{aligned} & v_p\left((na)!\,(nb)!\right) \\ &= v_p\left((na)!\right) + v_p\left((nb)!\right) = \sum_{i\geq 1}\left\lfloor \frac{na}{p^i}\right\rfloor + \sum_{i\geq 1}\left\lfloor \frac{nb}{p^i}\right\rfloor \qquad \text{(by Theorem 5.3.1)} \\ &= \sum_{i\geq 1}\left(\left\lfloor \frac{na}{p^i}\right\rfloor + \left\lfloor \frac{nb}{p^i}\right\rfloor\right). \end{aligned} \tag{14}$$

Hence, it will suffice to show that

$$\left\lfloor \frac{a}{p^i}\right\rfloor + \left\lfloor \frac{b}{p^i}\right\rfloor + (n-1)\left\lfloor \frac{a+b}{p^i}\right\rfloor \leq \left\lfloor \frac{na}{p^i}\right\rfloor + \left\lfloor \frac{nb}{p^i}\right\rfloor \tag{15}$$

for every positive integer i (because once this is proved, we can obtain (12) by summing (15) over all $i \in \{1,2,3,\ldots\}$).

In order to prove (15), we will show the following lemma:

Lemma 5.3.3. Let $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$. Then,

$$\lfloor x\rfloor + \lfloor y\rfloor + (n-1)\lfloor x+y\rfloor \leq \lfloor nx\rfloor + \lfloor ny\rfloor. \tag{16}$$

Proof of Lemma 5.3.3. We recall the following easy property of the floor function: If $r \in \mathbb{R}$ and $k \in \mathbb{Z}$, then

$$\lfloor r+k\rfloor = \lfloor r\rfloor + k. \tag{17}$$

(Convince yourself that this is true!)

Now, let $k \in \mathbb{Z}$ be arbitrary. Let us see what happens to the two sides of the inequality (16) if we replace x by $x+k$. Indeed, the left hand side becomes

$$\begin{aligned} & \lfloor x+k\rfloor + \lfloor y\rfloor + (n-1)\left\lfloor \underbrace{(x+k)+y}_{=x+y+k}\right\rfloor \\ &= \underbrace{\lfloor x+k\rfloor}_{\substack{=\lfloor x\rfloor + k \\ \text{(by (17), applied to } r=x\text{)}}} + \lfloor y\rfloor + (n-1)\underbrace{\lfloor x+y+k\rfloor}_{\substack{=\lfloor x+y\rfloor + k \\ \text{(by (17), applied to } r=x+y\text{)}}} \\ &= \lfloor x\rfloor + k + \lfloor y\rfloor + (n-1)\left(\lfloor x+y\rfloor + k\right) \\ &= \left(\lfloor x\rfloor + \lfloor y\rfloor + (n-1)\lfloor x+y\rfloor\right) + nk; \end{aligned}$$

in other words, the left hand side increases by nk. On the other hand, the right hand side of (16) becomes

$$\begin{aligned} \left\lfloor \underbrace{n(x+k)}_{=nx+nk}\right\rfloor + \lfloor ny\rfloor &= \underbrace{\lfloor nx+nk\rfloor}_{\substack{=\lfloor nx\rfloor + nk \\ \text{(by (17), applied to } nx \text{ and } nk \\ \text{instead of } r \text{ and } k\text{)}}} + \lfloor ny\rfloor \\ &= \lfloor nx\rfloor + nk + \lfloor ny\rfloor = \left(\lfloor nx\rfloor + \lfloor ny\rfloor\right) + nk; \end{aligned}$$

in other words, the right hand side also increases by nk. Thus, if we replace x by $x+k$, then both sides of (16) increase by one and the same amount (namely, by nk). Clearly, this increase does not change the validity of the inequality (16). Thus, we can replace x by $x+k$ without changing the validity of the inequality (16). Hence, for the rest of the proof of (16), we can WLOG assume that $0 \leq x < 1$, because we can always achieve this situation by replacing x by $x+k$ for an appropriate $k \in \mathbb{Z}$ (namely, for $k = -\lfloor x \rfloor$). Thus, let us WLOG assume that $0 \leq x < 1$. For similar reasons, we can WLOG assume that $0 \leq y < 1$. Let us assume this as well.

From $0 \leq x < 1$, we obtain $\lfloor x \rfloor = 0$. Similarly, $\lfloor y \rfloor = 0$. Thus, the inequality that we must prove – namely, (16) – simplifies to

$$(n-1)\lfloor x+y \rfloor \leq \lfloor nx \rfloor + \lfloor ny \rfloor . \tag{18}$$

From $0 \leq x$, we obtain $x \geq 0$ and thus $nx \geq 0$ (since $n \geq 0$). Hence, $\lfloor nx \rfloor \geq 0$ (because each real number $r \geq 0$ satisfies $\lfloor r \rfloor \geq 0$). Similarly, $\lfloor ny \rfloor \geq 0$. Thus, the right hand side of (18) is ≥ 0. Hence, (18) clearly holds if $\lfloor x+y \rfloor = 0$. For the rest of this proof, we thus WLOG assume that $\lfloor x+y \rfloor \neq 0$.

From $0 \leq x < 1$ and $0 \leq y < 1$, we obtain $0 \leq x+y < 2$. Thus, $\lfloor x+y \rfloor$ is either 0 or 1. Since $\lfloor x+y \rfloor \neq 0$, we thus obtain $\lfloor x+y \rfloor = 1$. Hence, $1 = \lfloor x+y \rfloor \leq x+y$ (since $\lfloor r \rfloor \leq r$ for each $r \in \mathbb{R}$), and thus $x+y \geq 1$.

However, it is well-known that $\lfloor r \rfloor > r-1$ for each $r \in \mathbb{R}$. Applying this to $r = nx$, we obtain $\lfloor nx \rfloor > nx-1$. Similarly, $\lfloor ny \rfloor > ny-1$. Adding these two inequalities together, we obtain

$$\lfloor nx \rfloor + \lfloor ny \rfloor > (nx-1) + (ny-1) = n\underbrace{(x+y)}_{\geq 1} - 2 \geq n-2.$$

Since $\lfloor nx \rfloor + \lfloor ny \rfloor$ and $n-2$ are integers, this entails $\lfloor nx \rfloor + \lfloor ny \rfloor \geq (n-2)+1 = n-1 = (n-1)\lfloor x+y \rfloor$ (because $\lfloor x+y \rfloor = 1$). In other words, $(n-1)\lfloor x+y \rfloor \leq \lfloor nx \rfloor + \lfloor ny \rfloor$. Thus, we have proved (18). Since (18) is an equivalent restatement of (16), we have therefore proved (16) as well. In other words, Lemma 5.3.3 is proved. □

The above proof of Lemma 5.3.3 illustrates a useful strategy (viz., transporting x into the interval $[0,1)$ by subtracting an appropriate integer).

Let us now return to solving Exercise 5.3.5 **(a)**. For each positive integer i, we

have

$$\begin{aligned}
&\left\lfloor \frac{a}{p^i} \right\rfloor + \left\lfloor \frac{b}{p^i} \right\rfloor + (n-1) \left\lfloor \frac{a+b}{p^i} \right\rfloor \\
&= \left\lfloor \frac{a}{p^i} \right\rfloor + \left\lfloor \frac{b}{p^i} \right\rfloor + (n-1) \left\lfloor \frac{a}{p^i} + \frac{b}{p^i} \right\rfloor \qquad \left(\text{since } \frac{a+b}{p^i} = \frac{a}{p^i} + \frac{b}{p^i} \right) \\
&\leq \left\lfloor n \cdot \frac{a}{p^i} \right\rfloor + \left\lfloor n \cdot \frac{b}{p^i} \right\rfloor \qquad \left(\begin{array}{c} \text{by Lemma 5.3.3,} \\ \text{applied to } x = \frac{a}{p^i} \text{ and } y = \frac{b}{p^i} \end{array} \right) \\
&= \left\lfloor \frac{na}{p^i} \right\rfloor + \left\lfloor \frac{nb}{p^i} \right\rfloor . \qquad (19)
\end{aligned}$$

Thus, (15) is proven. As explained above, this completes the proof of (12).

Now, forget that we fixed p. We thus have shown that each prime p satisfies (12). According to Proposition 5.2.11 (applied to $a!b!\,(a+b)!^{n-1}$ and $(na)!\,(nb)!$ instead of n and m), this entails that $a!b!\,(a+b)!^{n-1} \mid (na)!\,(nb)!$. Therefore, $\dfrac{(na)!\,(nb)!}{a!b!\,(a+b)!^{n-1}}$ is an integer. This solves Exercise 5.3.5 **(a)**.

(b) Let $m := \dfrac{(na)!\,(nb)!}{a!b!\,(a+b)!^{n-1}}$. We know from part **(a)** of this exercise that m is an integer. We must show that m is divisible by n. In other words, we must show that $n \mid m$. According to Proposition 5.2.11, it suffices to show that each prime p satisfies $v_p(n) \leq v_p(m)$.

So let p be a prime. Our goal is to show that $v_p(n) \leq v_p(m)$. In other words, our goal is to show that $v_p(m) \geq v_p(n)$.

From $m = \dfrac{(na)!\,(nb)!}{a!b!\,(a+b)!^{n-1}}$, we obtain $m \cdot a!b!\,(a+b)!^{n-1} = (na)!\,(nb)!$, so that

$$\begin{aligned}
&v_p\left(m \cdot a!b!\,(a+b)!^{n-1} \right) \\
&= v_p\left((na)!\,(nb)! \right) = \sum_{i \geq 1} \left(\left\lfloor \frac{na}{p^i} \right\rfloor + \left\lfloor \frac{nb}{p^i} \right\rfloor \right) \qquad \text{(by (14))}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\sum_{i \geq 1} \left(\left\lfloor \frac{na}{p^i} \right\rfloor + \left\lfloor \frac{nb}{p^i} \right\rfloor \right) \\
&= v_p\left(m \cdot a!b!\,(a+b)!^{n-1} \right) \\
&= v_p(m) + v_p\left(a!b!\,(a+b)!^{n-1} \right) \qquad \text{(by Theorem 5.2.5 \textbf{(a)})} \\
&= v_p(m) + \sum_{i \geq 1} \left(\left\lfloor \frac{a}{p^i} \right\rfloor + \left\lfloor \frac{b}{p^i} \right\rfloor + (n-1) \left\lfloor \frac{a+b}{p^i} \right\rfloor \right)
\end{aligned}$$

(by (13)). Solving this equation for $v_p(m)$, we obtain

$$\begin{aligned} & v_p(m) \\ &= \sum_{i \geq 1} \left(\left\lfloor \frac{na}{p^i} \right\rfloor + \left\lfloor \frac{nb}{p^i} \right\rfloor \right) - \sum_{i \geq 1} \left(\left\lfloor \frac{a}{p^i} \right\rfloor + \left\lfloor \frac{b}{p^i} \right\rfloor + (n-1) \left\lfloor \frac{a+b}{p^i} \right\rfloor \right) \\ &= \sum_{i \geq 1} \left(\left\lfloor \frac{na}{p^i} \right\rfloor + \left\lfloor \frac{nb}{p^i} \right\rfloor - \left(\left\lfloor \frac{a}{p^i} \right\rfloor + \left\lfloor \frac{b}{p^i} \right\rfloor + (n-1) \left\lfloor \frac{a+b}{p^i} \right\rfloor \right) \right). \end{aligned} \tag{20}$$

Thus, we need to show that the sum on the right hand side is $\geq v_p(n)$ (since our goal is to show that $v_p(m) \geq v_p(n)$). The inequality (19) shows that each addend in this sum is ≥ 0; thus, it will suffice to show that at least $v_p(n)$ many of these addends are ≥ 1 each.

This is what we shall now do. To be specific, we set $h := \min\left\{v_p(a), v_p(b)\right\}$; this is a nonnegative integer (since $(a,b) \neq (0,0)$ entails that at least one of $v_p(a)$ and $v_p(b)$ belongs to $\mathbb{N}$). We will now show that each $i \in \left\{h+1, h+2, \ldots, h+v_p(n)\right\}$ satisfies

$$\left\lfloor \frac{na}{p^i} \right\rfloor + \left\lfloor \frac{nb}{p^i} \right\rfloor - \left(\left\lfloor \frac{a}{p^i} \right\rfloor + \left\lfloor \frac{b}{p^i} \right\rfloor + (n-1) \left\lfloor \frac{a+b}{p^i} \right\rfloor \right) \geq 1. \tag{21}$$

[*Proof of (21):* Let $i \in \left\{h+1, h+2, \ldots, h+v_p(n)\right\}$. Thus, $h < i \leq h + v_p(n)$.

We have $h = \min\left\{v_p(a), v_p(b)\right\} \leq v_p(a)$ and

$$i \leq \underbrace{h}_{\leq v_p(a)} + v_p(n) \leq v_p(a) + v_p(n) = v_p(n) + v_p(a) = v_p(na)$$

(since Theorem 5.2.5 **(a)** yields $v_p(na) = v_p(n) + v_p(a)$). In other words, $v_p(na) \geq i$. However, Lemma 5.2.3 (applied to na instead of n) yields that $p^i \mid na$ if and only if $v_p(na) \geq i$. Hence, $p^i \mid na$ (since $v_p(na) \geq i$). Thus, $\dfrac{na}{p^i}$ is an integer, so that $\left\lfloor \dfrac{na}{p^i} \right\rfloor = \dfrac{na}{p^i}$ (since $\lfloor r \rfloor = r$ for every integer r). Similarly, $\left\lfloor \dfrac{nb}{p^i} \right\rfloor = \dfrac{nb}{p^i}$.

We note that a and b play symmetric roles in our claim. Thus, we can WLOG assume that $v_p(a) \leq v_p(b)$ (since otherwise, we can just swap a with b). Hence, $h = \min\left\{v_p(a), v_p(b)\right\} = v_p(a)$ (since $v_p(a) \leq v_p(b)$). Hence, the inequality $h < i$ (which we know to hold) rewrites as $v_p(a) < i$. In other words, we don't have $v_p(a) \geq i$. However, Lemma 5.2.3 (applied to a instead of n) yields that $p^i \mid a$ if and only if $v_p(a) \geq i$. Hence, we don't have $p^i \mid a$ (since we don't have $v_p(a) \geq i$). In other words, $\dfrac{a}{p^i}$ is not an integer. Thus, $\left\lfloor \dfrac{a}{p^i} \right\rfloor < \dfrac{a}{p^i}$ (because if $r \in \mathbb{R}$ is not an integer, then $\lfloor r \rfloor < r$).

Also, recall that any $r \in \mathbb{R}$ satisfies $\lfloor r \rfloor \leq r$. Hence, $\left\lfloor \dfrac{b}{p^i} \right\rfloor \leq \dfrac{b}{p^i}$ and $\left\lfloor \dfrac{a+b}{p^i} \right\rfloor \leq \dfrac{a+b}{p^i}$. We can multiply the latter inequality by $n-1$ (indeed, $n-1 \geq 0$, because n is a positive integer), and thus obtain $(n-1)\left\lfloor \dfrac{a+b}{p^i} \right\rfloor \leq (n-1)\dfrac{a+b}{p^i}$.

Now, using all the equalities and inequalities we have proved so far, we see that

$$\begin{aligned}
&\underbrace{\left\lfloor \frac{na}{p^i} \right\rfloor}_{=\frac{na}{p^i}} + \underbrace{\left\lfloor \frac{nb}{p^i} \right\rfloor}_{=\frac{nb}{p^i}} - \left(\underbrace{\left\lfloor \frac{a}{p^i} \right\rfloor}_{<\frac{a}{p^i}} + \underbrace{\left\lfloor \frac{b}{p^i} \right\rfloor}_{\leq \frac{b}{p^i}} + \underbrace{(n-1) \left\lfloor \frac{a+b}{p^i} \right\rfloor}_{\leq (n-1)\frac{a+b}{p^i}} \right) \\
&> \frac{na}{p^i} + \frac{nb}{p^i} - \left(\frac{a}{p^i} + \frac{b}{p^i} + (n-1) \frac{a+b}{p^i} \right) = 0.
\end{aligned}$$

Since $\left\lfloor \frac{na}{p^i} \right\rfloor + \left\lfloor \frac{nb}{p^i} \right\rfloor - \left(\left\lfloor \frac{a}{p^i} \right\rfloor + \left\lfloor \frac{b}{p^i} \right\rfloor + (n-1) \left\lfloor \frac{a+b}{p^i} \right\rfloor \right)$ is an integer, this entails

$$\left\lfloor \frac{na}{p^i} \right\rfloor + \left\lfloor \frac{nb}{p^i} \right\rfloor - \left(\left\lfloor \frac{a}{p^i} \right\rfloor + \left\lfloor \frac{b}{p^i} \right\rfloor + (n-1) \left\lfloor \frac{a+b}{p^i} \right\rfloor \right) \geq 1.$$

Thus, (21) is proved.]

Now, we are almost there: We know that all addends in the sum on the right hand side of (20) are nonnegative (by (19)), and we also know that at least $v_p(n)$ many of these addends are ≥ 1 each (indeed, (21) shows that the addends for $i \in \{h+1, h+2, \ldots, h+v_p(n)\}$ are ≥ 1 each). Thus, the entire sum is $\geq \underbrace{1+1+\cdots+1}_{v_p(n) \text{ times}} = v_p(n)$. Hence, the left hand side of (20) is also $\geq v_p(n)$. In other words, we have $v_p(m) \geq v_p(n)$. But proving this inequality was precisely our goal. Thus, we have solved Exercise 5.3.5 **(b)**. □

5.4. Class problems

The following problems are to be discussed during class.

Exercise 5.4.1. Let $n \in \mathbb{N}$. Let a and b be two coprime positive integers. Assume that ab is the n-th power of a positive integer. Prove that a and b are n-th powers of positive integers.

Exercise 5.4.2. Let a and b be two integers. Let $i \in \mathbb{N}$ be such that $2^i > |b|$. Assume that $a^i \mid b^{i+1}$. Show that $a \mid b$.

Exercise 5.4.3. With how many 0s does the base-10 representation of the number 90! end?

Exercise 5.4.4. Let $a \in \mathbb{Z}$, and let n be a positive integer. Prove that

$$n! \mid a^{n-1} \prod_{i=1}^{n} \left(a^i - 1\right).$$

Exercise 5.4.5. Let p be a prime. Let a and b be two integers such that $a \equiv b \not\equiv 0 \bmod p$. Let n be a positive integer.

(a) Prove that $v_p\left(a^n - b^n\right) \geq v_p\left(a-b\right) + v_p\left(n\right)$.

(b) Prove that $v_p\left(a^n - b^n\right) = v_p\left(a-b\right) + v_p\left(n\right)$ if $p \neq 2$.

(c) Prove that $v_p\left(a^n - b^n\right) = v_p\left(a-b\right) + v_p\left(n\right)$ if $p = 2$ and $a \equiv b \bmod 4$.

(d) Find an example where $p = 2$ and $a \equiv b \bmod 2$ and $v_p\left(a^n - b^n\right) > v_p\left(a-b\right) + v_p\left(n\right)$.

5.5. Homework exercises

Solve 3 of the 6 exercises below and upload your solutions on gradescope by October 29.

Exercise 5.5.1. Let $a, b, c \in \mathbb{Z}$. Prove that:

(a) We have

$$\gcd\left(b,c\right) \cdot \gcd\left(c,a\right) \cdot \gcd\left(a,b\right) = \gcd\left(a,b,c\right) \cdot \gcd\left(bc,ca,ab\right).$$

(b) We have

$$\operatorname{lcm}\left(b,c\right) \cdot \operatorname{lcm}\left(c,a\right) \cdot \operatorname{lcm}\left(a,b\right) = \operatorname{lcm}\left(a,b,c\right) \cdot \operatorname{lcm}\left(bc,ca,ab\right).$$

(c) Assume that a, b, c are nonzero. Then,

$$\frac{\gcd\left(bc,ca,ab\right)}{\gcd\left(a,b,c\right)} = \frac{\operatorname{lcm}\left(bc,ca,ab\right)}{\operatorname{lcm}\left(a,b,c\right)} \in \mathbb{Z}.$$

Exercise 5.5.2. Fix a prime p. Let a and b be two integers satisfying $\gcd\left(a,b\right) = p$. What values can $\gcd\left(a^5, b^{13}\right)$ take?

Exercise 5.5.3. Let $n, a, b, c \in \mathbb{N}$ such that n is odd. Prove that

$$\frac{\left(na\right)!\left(nb\right)!\left(nc\right)!}{a!b!c!\left(\left(b+c\right)!\left(c+a\right)!\left(a+b\right)!\right)^{\left(n-1\right)/2}}$$

is an integer.

Exercise 5.5.4. Let $n \in \mathbb{N}$. Prove that

$$(n+1)\operatorname{lcm}\left(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}\right) = \operatorname{lcm}(1,2,\ldots,n+1).$$

Exercise 5.5.5. Let k and n be any two positive integers. Prove that an expression of the form

$$\pm\frac{1}{k} \pm \frac{1}{k+1} \pm \frac{1}{k+2} \pm \cdots \pm \frac{1}{k+n}$$

(where each $\pm$ sign is either a $+$ or a $-$ sign) will never be an integer, no matter what the $\pm$ signs are.

[**Hint:** Show that one of the numbers $k, k+1, \ldots, k+n$ has a higher 2-valuation than all of the others.]

Exercise 5.5.6. Let $(u_1, u_2, u_3, \ldots)$ be a sequence of nonzero integers such that

$$\text{every } a,b \in \{1,2,3,\ldots\} \text{ satisfy } \gcd(u_a, u_b) = \left|u_{\gcd(a,b)}\right|.$$

(We have seen such a sequence in Exercise 3.7.4; another example is the Fibonacci sequence because of [Grinbe20, Exercise 3.7.2].)

Prove that there exists a sequence $(v_1, v_2, v_3, \ldots)$ of nonzero integers such that

$$\text{each } n \in \{1,2,3,\ldots\} \text{ satisfies } u_n = \prod_{d \mid n} v_d.$$

Here, the symbol "$\prod_{d \mid n}$" means a product over all positive divisors d of n. Thus, the equality $u_n = \prod_{d \mid n} v_d$ means

$$\begin{aligned}
u_1 &= v_1 && \text{for } n = 1;\\
u_2 &= v_1 v_2 && \text{for } n = 2;\\
u_3 &= v_1 v_3 && \text{for } n = 3;\\
u_4 &= v_1 v_2 v_4 && \text{for } n = 4;\\
u_5 &= v_1 v_5 && \text{for } n = 5;\\
u_6 &= v_1 v_2 v_3 v_6 && \text{for } n = 6;
\end{aligned}$$

and so on.

Exercise 5.5.7. Prove that $\gcd(a,b) = \gcd(a+b, \operatorname{lcm}(a,b))$ for any two integers a and b.

5.6. Appendix: Proof of Proposition 5.2.15

We shall now prove Proposition 5.2.15. First, we recall the universal properties of gcds and lcms:

Theorem 5.6.1 (universal properties of gcd and lcm)**.** Let $b_1, b_2, \ldots, b_k$ be integers. Let $m \in \mathbb{Z}$.

(a) We have the following logical equivalence:

$$(m \mid b_i \text{ for all } i \in \{1,2,\ldots,k\}) \iff (m \mid \gcd(b_1, b_2, \ldots, b_k)).$$

(b) We have the following logical equivalence:

$$(b_i \mid m \text{ for all } i \in \{1,2,\ldots,k\}) \iff (\operatorname{lcm}(b_1, b_2, \ldots, b_k) \mid m).$$

So Theorem 5.6.1 **(a)** says that the common divisors of k integers $b_1, b_2, \ldots, b_k$ are precisely the divisors of $\gcd(b_1, b_2, \ldots, b_k)$; meanwhile, Theorem 5.6.1 **(b)** says that the common multiples of k integers $b_1, b_2, \ldots, b_k$ are precisely the multiples of $\operatorname{lcm}(b_1, b_2, \ldots, b_k)$.

Theorem 5.6.1 **(a)** is proved in [Grinbe19, Theorem 2.9.21 **(a)**]. Theorem 5.6.1 **(b)** is proved in [Grinbe19, Theorem 2.11.9 **(a)**].

Proof of Proposition 5.2.15 (sketched). **(a)** We WLOG assume that the k integers $n_1, n_2, \ldots, n_k$ are not all equal to 0 (since otherwise, the claim boils down to $\infty = \min\{\infty, \infty, \ldots, \infty\}$). Thus, $\min\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\}$ is a nonnegative integer (not ∞).

Let $g = \gcd(n_1, n_2, \ldots, n_k)$. Then, g is a positive integer (since $n_1, n_2, \ldots, n_k$ are not all equal to 0). Hence, $v_p(g)$ is a nonnegative integer (not ∞).

For each $i \in \{1,2,\ldots,k\}$, we have $g = \gcd(n_1, n_2, \ldots, n_k) \mid n_i$ (by the definition of the gcd) and thus $v_p(g) \leq v_p(n_i)$ (by Proposition 5.2.11, applied to $n = g$ and $m = n_i$). Hence,

$$v_p(g) \leq \min\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\} \tag{22}$$

(since $\min\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\} = v_p(n_i)$ for some $i \in \{1,2,\ldots,k\}$).

Now, assume (for the sake of contradiction) that the inequality (22) is strict (i.e., not an equality). Thus,

$$v_p(g) < \min\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\}. \tag{23}$$

Let $i \in \{1,2,\ldots,k\}$. Then, (23) becomes

$$\begin{aligned} v_p(g) &< \min\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\} \\ &\leq v_p(n_i). \end{aligned} \tag{24}$$

However, $g = \gcd(n_1, n_2, \ldots, n_k) \mid n_i$ (by the definition of the gcd), so that $\frac{n_i}{g} \in \mathbb{Z}$ (since g is a positive integer). Theorem 5.2.5 **(a)** yields $v_p\left(g \cdot \frac{n_i}{g}\right) = v_p(g) + v_p\left(\frac{n_i}{g}\right)$, so that

$$v_p\left(\frac{n_i}{g}\right) = v_p\left(\underbrace{g \cdot \frac{n_i}{g}}_{=n_i}\right) - \underbrace{v_p(g)}_{\substack{<v_p(n_i) \\ \text{(by (24))}}} > v_p(n_i) - v_p(n_i) = 0.$$

Thus, we don't have $v_p\left(\frac{n_i}{g}\right) = 0$. However, Corollary 5.2.4 (applied to $n = \frac{n_i}{g}$) yields that $v_p\left(\frac{n_i}{g}\right) = 0$ if and only if $p \nmid \frac{n_i}{g}$. Hence, we don't have $p \nmid \frac{n_i}{g}$ (since we don't have $v_p\left(\frac{n_i}{g}\right) = 0$). In other words, we have $p \mid \frac{n_i}{g}$. Hence, $\frac{n_i}{g}/p \in \mathbb{Z}$. In other words, $\frac{n_i}{pg} \in \mathbb{Z}$ (since $\frac{n_i}{g}/p = \frac{n_i}{pg}$). In other words, $pg \mid n_i$.

Forget that we fixed i. We thus have shown that $pg \mid n_i$ for all $i \in \{1, 2, \ldots, k\}$. However, Theorem 5.6.1 **(a)** (applied to $b_i = n_i$ and $m = pg$) shows that this is equivalent to having $pg \mid \gcd(n_1, n_2, \ldots, n_k)$. Thus, we obtain $pg \mid \gcd(n_1, n_2, \ldots, n_k)$. In view of $\gcd(n_1, n_2, \ldots, n_k) = g$, this rewrites as $pg \mid g$. Hence, $\frac{g}{pg} \in \mathbb{Z}$. But this contradicts $\frac{g}{pg} = \frac{1}{p} \notin \mathbb{Z}$. This contradiction shows that our assumption (viz., that the inequality (22) is strict) was false. Hence, the inequality (22) cannot be strict, i.e., must be an equality. In other words, we have

$$v_p(g) = \min\left\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\right\}.$$

In view of $g = \gcd(n_1, n_2, \ldots, n_k)$, this rewrites as

$$v_p(\gcd(n_1, n_2, \ldots, n_k)) = \min\left\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\right\}.$$

Thus, Proposition 5.2.15 **(a)** is proved. (A different proof can be found in [Grinbe20, proof of Proposition 9.3.11].)

(b) We WLOG assume that none of the k integers $n_1, n_2, \ldots, n_k$ equals 0 (since otherwise, the claim boils down to $\infty = \max S$ for a set S that contains ∞). Thus, $\max\left\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\right\}$ is a nonnegative integer (not ∞).

Let $\ell = \operatorname{lcm}(n_1, n_2, \ldots, n_k)$. Then, ℓ is a positive integer (since none of $n_1, n_2, \ldots, n_k$ equals 0). Hence, $v_p(\ell)$ is a nonnegative integer (not ∞).

For each $i \in \{1, 2, \ldots, k\}$, we have

$$n_i \mid \ell \tag{25}$$

(because the definition of an lcm yields $n_i \mid \operatorname{lcm}(n_1, n_2, \ldots, n_k) = \ell$) and thus $v_p(n_i) \leq v_p(\ell)$ (by Proposition 5.2.11, applied to $n = n_i$ and $m = \ell$). In other words, for each $i \in \{1, 2, \ldots, k\}$, we have $v_p(\ell) \geq v_p(n_i)$. Hence,

$$v_p(\ell) \geq \max\left\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\right\} \tag{26}$$

(since $\max\left\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\right\} = v_p(n_i)$ for some $i \in \{1, 2, \ldots, k\}$).

Now, assume (for the sake of contradiction) that the inequality (26) is strict (i.e., not an equality). Thus,

$$v_p(\ell) > \max\left\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\right\}. \tag{27}$$

Hence, $v_p(\ell) > \max\left\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\right\} \geq 0$. Thus, we don't have $v_p(\ell) = 0$. However, Corollary 5.2.4 (applied to $n = \ell$) yields that $v_p(\ell) = 0$ if and only if $p \nmid \ell$. Hence, we don't have $p \nmid \ell$ (since we don't have $v_p(\ell) = 0$). In other words, we have $p \mid \ell$. Hence, $\ell/p \in \mathbb{Z}$.

Let $i \in \{1, 2, \ldots, k\}$. Then, (27) becomes

$$\begin{aligned} v_p(\ell) &> \max\left\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\right\} \\ &\geq v_p(n_i). \end{aligned} \tag{28}$$

Furthermore, $n_i \mid \ell$ (by (25)), so that $\dfrac{\ell}{n_i} \in \mathbb{Z}$ (since $n_i \neq 0$ (because none of $n_1, n_2, \ldots, n_k$ equals 0)). Theorem 5.2.5 **(a)** yields $v_p\left(n_i \cdot \dfrac{\ell}{n_i}\right) = v_p(n_i) + v_p\left(\dfrac{\ell}{n_i}\right)$, so that

$$v_p\left(\frac{\ell}{n_i}\right) = v_p\left(\underbrace{n_i \cdot \frac{\ell}{n_i}}_{=\ell}\right) - v_p(n_i) = \underbrace{v_p(\ell)}_{\substack{> v_p(n_i) \\ \text{(by (28))}}} - v_p(n_i) > v_p(n_i) - v_p(n_i) = 0.$$

Thus, we don't have $v_p\left(\dfrac{\ell}{n_i}\right) = 0$. However, Corollary 5.2.4 (applied to $n = \dfrac{\ell}{n_i}$) yields that $v_p\left(\dfrac{\ell}{n_i}\right) = 0$ if and only if $p \nmid \dfrac{\ell}{n_i}$. Hence, we don't have $p \nmid \dfrac{\ell}{n_i}$ (since we don't have $v_p\left(\dfrac{\ell}{n_i}\right) = 0$). In other words, we have $p \mid \dfrac{\ell}{n_i}$. Hence, $\dfrac{\ell}{n_i}/p \in \mathbb{Z}$. In other words, $\dfrac{\ell/p}{n_i} \in \mathbb{Z}$ (since $\dfrac{\ell}{n_i}/p = \dfrac{\ell/p}{n_i}$). In other words, $n_i \mid \ell/p$ (since $\ell/p \in \mathbb{Z}$).

Forget that we fixed i. We thus have shown that $n_i \mid \ell/p$ for all $i \in \{1, 2, \ldots, k\}$. However, Theorem 5.6.1 **(b)** (applied to $b_i = n_i$ and $m = \ell/p$) shows that this is equivalent to $\operatorname{lcm}(n_1, n_2, \ldots, n_k) \mid \ell/p$ (since $\ell/p \in \mathbb{Z}$). Thus, we obtain $\operatorname{lcm}(n_1, n_2, \ldots, n_k) \mid \ell/p$. In view of $\operatorname{lcm}(n_1, n_2, \ldots, n_k) = \ell$, this rewrites as $\ell \mid \ell/p$.

Hence, $\dfrac{\ell/p}{\ell} \in \mathbb{Z}$ (since ℓ is positive). But this contradicts $\dfrac{\ell/p}{\ell} = \dfrac{1}{p} \notin \mathbb{Z}$. This contradiction shows that our assumption (viz., that the inequality (26) is strict) was false. Hence, the inequality (26) cannot be strict, i.e., must be an equality. In other words, we have

$$v_p(\ell) = \max\left\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\right\}.$$

In view of $\ell = \operatorname{lcm}(n_1, n_2, \ldots, n_k)$, this rewrites as

$$v_p(\operatorname{lcm}(n_1, n_2, \ldots, n_k)) = \max\left\{v_p(n_1), v_p(n_2), \ldots, v_p(n_k)\right\}.$$

Thus, Proposition 5.2.15 **(b)** is proved. □

References

[Grinbe19] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 1 October 2020.
`http://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf`

[Grinbe20] Darij Grinberg, *Math 235: Mathematical Problem Solving*, 10 August 2021.
`https://www.cip.ifi.lmu.de/~grinberg/t/20f/mps.pdf`